5239
63D
18 Sep 98

From: Commander, Naval Supply Systems Command

Subj: NAVAL SUPPLY SYSTEMS COMMAND ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE (PKI) POLICY FOR SENSITIVE BUT UNCLASSIFIED (SBU) SYSTEMS

Ref: (a) NAVSUP ltr 5239 63D of 16 Jan 98
(b) DOD Memo of 16 Aug 98 (NOTAL)

Encl: (1) INFOSEC Policy and Procedures for SBU Data Transmitted Via the Internet
(2) Definition of Terms

1. With the increased availability of Web browsers, many NAVSUP business managers are Web-enabling their SBU data applications to conduct business via the Internet. Reference (a) sets forth NAVSUP Information Systems Security (INFOSEC) requirements for protection of Web sites. This letter forwards the INFOSEC policy and procedures for protecting SBU data being transmitted via the Internet.

2. NAVSUP INFOSEC requirements for protecting the data, i.e., encrypting the data during transmission and authenticating the user by issuing digital certificates via a PKI, are attached as enclosure (1). All NAVSUP business managers of Web-enabled applications processing SBU data via the Internet shall comply with these requirements. Enclosure (2) is provided for the understanding of architectural terms and government standards.

3. The NAVSUP INFOSEC Program Office is coordinating a parallel DOD PKI effort, as outlined in reference (b), and is taking the necessary steps to migrate the current architecture to the DOD PKI, when appropriate.

4. NAVSUP point of contact is Charlene F. Tallman, SUP 63D, at 717-605-1432 (DSN 430).

/s/ J.D. FINCH
By direction

Subj: NAVAL SUPPLY SYSTEMS COMMAND ENCRYPTION AND PUBLIC KEY
INFRASTRUCTURE (PKI) POLICY FOR SENSITIVE BUT
UNCLASSIFIED (SBU) SYSTEMS

Distribution:
FHSO (Code 00)
FISC Jacksonville (Code CO)
FISC Norfolk (Code 00)
FISC Oakland (Code 00)
FISC Pearl Harbor (Code 00)
FISC Puget Sound (Code 00)
FISC San Diego (Code 00)
FISC Yokosuka (Code 00)
FMSO (Code 9)
FOSSAC (Code 00)
NAVICP (Code 00)
NAVPETOFF (Code 00)
NAVTRANS (Code 00)
NCTRF (Code 00)
NEXCOM (Code 00)

Copy to:
FHSO (Code 05221)
FISC Jacksonville (Code 3OX)
FISC Norfolk (Code 12)
FISC Oakland (Code 91.lAC)
FISC Pearl Harbor (Code 928)
FISC Puget Sound (Code 43.2)
FISC San Diego (Code 3l)
FISC Yokosuka (Codes 00, 35)
FMSO (Code 941-ASAT, 94E, 941, 95B, 961)
FOSSAC (Code 01C)
NAVICP (Codes 041, 0416, 054, 0542, 05422.03, 0543, 05733,
M0433.01, P045.25, P089, P0892, M0891.03, P08921.02)
NAVPETOFF (Code 10)
NAVSUP (X32 and Codes 02XB, 33C, ED-1A, ED-12B)
NAVTRANS (Code 06)
NCTRF (Code N3.SS)
NEXCOM (Code IA)

INFOSEC Policy and Procedures for SBU Data Transmitted Via the Internet

Ref: (a) DODINST 5200.40 of 30 Dec 97

1. The NAVSUP INFOSEC Program Office has joined efforts with the Naval Sea and Air Systems Commands in a one-year Navy Acquisition PKI Pilot. The Navy Acquisition PKI Pilot architecture encrypts the data during transmission so the data cannot be seen in the clear and issues digital certificates, via a PKI, to authenticate the user ensuring only subscribers with a need-to-know have access to the data. This architecture complies with the required FIPS 140-1 encryption and X.509 Version 3 certificate government standards.

2. The Certificate Practice Statement for the Navy Acquisition PKI Pilot identifies policy and guidelines. This policy can be found at Uniform Resource Locator (URL) www.pki.navy.mil. It is the responsibility of each NAVSUP subscriber and Registration Authority (RA) of this architecture to read and comply with its mandates.

3. The Navy Acquisition PKI Pilot covers a one-year period beginning 30 March 1998, and applies to NAVSUP claimancy, as well as to all contractors, foreign nationals, and organizations supporting NAVSUP SBU-application efforts. This date may be extended if migration to the DOD PKI does not occur before 30 March 1999.

4. The following paragraphs address NAVSUP-specific PKI policy, an explanation of the NAVSUP PKI hierarchy architecture, NAVSUP resources required to perform the function, and outlines the process to acquire the secure browser and a digital certificate. Specifically,

a. NAVSUP-Specific PKI Policy.

(1) The "owner" of the data/application is responsible for determining the data level of classification. i.e., unclassified or sensitive but unclassified.

(2) Any NAVSUP Program Manager utilizing the Navy Acquisition PKI for his/her SBU application shall accredit his/her system, per reference (a), prior to operation. If the system is not accredited, an Interim Authority To Operate (IATO) shall be issued and provided to the NAVSUP INFOSEC Program Office. This IATO shall allow system operations to continue while performing the accreditation process. The IATO may not exceed a period of one year.

(3) If the application Web site provides access to other disparate databases/Web sites behind the Web site, the Program Manager shall negotiate a Memorandum of Understanding with the database/Web site owner outlining the INFOSEC services provided

and negotiate mutually-agreed upon terms and responsibilities.

(4) NAVSUP digital certificate subscriber RA step-by-step instructions are enclosed as Attachments (A) and (B), respectively. These instructions can also be found at URL www.pki.navy.mil. It is the responsibility of each NAVSUP subscriber and RA of this architecture to read and comply with its mandates. NAVSUP-specific subscriber and RA instructions follow.

a) All digital certificate subscribers will be responsible for memorizing and securing their password to their private key on the digital certificate which, in most cases, will reside on their hard drive encrypted. If a hard drive containing a digital certificate must be returned, for any reason to the Information Center, it is the responsibility of the subscriber to ensure the hard drive is written over three times by Norton Utilities, or the like, to minimize the possibility of password compromise.

b) If a subscriber is processing requisitions via the Internet over $100K, additional security requirements shall be required. Contact the NAVSUP INFOSEC POC for additional information.

c) Compliance with certificate revocation procedures is required. The procedures are annotated as part of Attachments (A) and (B).

d) Compliance with certificate expiration procedures is required. The shelf life of a digital certificate is annotated as a part of Attachments (A) and (B).

b. The Architecture.

(1) The SBU architecture consists of two pieces: (1) encrypting the data so it is not seen in the clear and (2) authenticating the subscriber via a digital certificate.

a) Data Encryption. The secure version of the browser client to the Web server automatically provides a secure sockets layer (SSL) encrypting the data. Federal Information Processing Standards (FIPS) 140-1 is the government encryption standard. Today only Netscape's browser (U.S. Security version) is compliant. The secure browser may be acquired by visiting URL www.pki.navy.mil.

b) Subscriber Authentication. Today, most applications authenticate subscribers via a password and activity identification code. The state-of-the-art electronic version of this step is a digital certificate via a PKI. There are three pieces involved with PKI: (1) the subscriber requesting a digital certificate, (2) the RA authenticating the subscriber to the Certificate Authority (CA), and (3) CA issuing the digital certificate to the subscriber.

1) The Subscriber. The subscriber is a government employee, or a contractor, or a foreign national, or an organization supporting the government that has a “need to know” and can prove authenticity to the RA.

NAVSUP Resources Required: None.

2) The RA. The Registration Authority is the person at NAVSUP Headquarters, or the local site, or onboard ship, to whom a digital certificate has been issued AND to whom a subscriber must communicate with to obtain authentication. Within the NAVSUP Claimancy, an already-established infrastructure will be used, i.e., a local site's Activity Approval Authority (AAA). The AAA, i.e., RA, will communicate with a subscriber's supervisor, another individual who knows the subscriber, or by face-to-face contact, validating the subscriber’s authenticity and approving the request for a digital certificate.

NAVSUP Resources Required: No additional resources are required. The local infrastructure in place today will be utilized.

3) The CA. Within the established Navy Acquisition PKI architecture hierarchy, the Navy has delegated the capability for each SYSCOM to have their own root CA. Under NAVSUP's root CA, NAVSUP is delegating each site a SITE CA. These CAs reside on a certificate server and the CA function is performed electronically. With this architecture, a thread of trust is established between the Navy CA, the NAVSUPSYSCOM root CA, the SITE CA, and the subscriber via a secure Web browser.

NAVSUP Resources Required: None required today. For the PKI pilot, CA functions have been out-sourced. As the Claimancy becomes more proficient in the applying for, approving of, and granting thereof of digital certificates, CAs may be delegated to SYSCOM/SITE/SHIP, i.e., sites will migrate into this function.

c. The Process.

(1) After acquiring a FIPS 140-1 compliant browser, a subscriber applies for a digital certificate to access a SBU application that requires a Navy Acquisition digital certificate. The subscriber follows the step-by-step subscriber instructions attached, or located at URL www.pki.navy.mil, to acquire a digital certificate.

(2) The RA, who already has a digital certificate and is part of the PKI, is electronically notified of the digital certificate request via email. The RA follows the step-by-step Registration Authority Instructions attached, or located at URL

www.pki.navy.mil, validating the subscriber and then approves the request and forwards it to the CA for issuance.

(3) The CA receives the approval request from the site RA, issues the digital certificate, and emails the subscriber specific directions on where and how to download the digital certificate onto his/her hard drive.

(4) For the sailor in port or at sea who must acquire a digital certificate, an RA onboard ship shall be designated and trained to maintain the thread of thrust being established by this hierarchy.

DEFINITION OF TERMS

FIPS 140-1:

FIPS (Federal Information Processing Standards) 140-1 designates a standard entitled "Security Requirements for Cryptographic Modules". It is the set of standards developed by the U.S. National Institute of Standards and Technology (NIST) to lay out requirements for cryptographic modules within computer and telecommunication systems.

PKI:

Public Key Infrastructure (PKI) is a system of digital certificates, Certificate Authorities (CA), and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction using key pairs called public-and-private keys.

A digital certificate is a digital document that vouches for the identity and key ownership of an individual, a computer system, or a server running on that system, or an organization. Personal certificates serve two purposes: (1) they make a subscriber's personal "public key" available to other people and (2) they "certify" identity of the subscriber.

Certificates are issued by Certificate Authorities (CAs). CAs are trusted authorities who, via this process, "certify" that you are. CAs also "certify" that you own a specific public key. In addition to issuing certificates, CAs can also revoke certificates.

SBU:

The Computer Security Act of 1987 is the Federal document that states Sensitive But Unclassified data (SBU) in federal computer systems (including contractor that support government initiatives) will be protected to government standards. This congressional act sanctions FIPS to define requirements for automated information systems and establishes these requirements as binding on U. S. Government agencies.

There are nine categories of SBU which are described below:

Data Category

Description

Proprietary Data

Trade secrets and commercial or Financial information obtained from a Person and privileged or Confidential.

For official Use Only

Categories of information exempt from Public release under the provisions of the Freedom of Information Act (FOIA). Documents containing FOIA exempt information are identified by the caveat "For official Use Only."

Treaties & International Agreements

Information which must be protected in accordance with the stipulations of a particular treaty or international agreement such as the Chemical Weapons Compliance Treaty or North American Free Trade Agreement.

Technical Military Data

Technical data with military or space application which may not be exported lawfully outside the U.S. without prior approval, authorization, or license under the Export Act of 1979 or the Arms Export Control Act.

Export Control Data

Data which is subject to export controls (international traffic in arms regulation, export control act, U.S. munitions list).

Competition Sensitive Data

Data associated with ongoing procurement of government supplies, services or equipment to include contractor bids and proposals and associated government documents.

Privacy Act

Information which must be protected from public release to protect the privacy of the individual (social security number, investigative data, payroll records, disciplinary records, etc.).

Investigative and Inquiry Data

Information associated with or resulting from criminal, civil, security, inspector general, flight safety, or other investigations or inquiries which must be protected from public release.

Naval Nuclear Propulsion Information

Information concerning the design and operation of Naval nuclear reactors and associated equipment which does not meet the criteria for classification under Executive Order

In the absence of the DOD/Navy policy mandating all logistical information is considered SBU, NAVSUP policy states that the “owner" of the data/application determines the data classification and is the responsible party.